INTEGRAL BASES IN KUMMER EXTENSIONS OF DEDEKIND FIELDS

LEON R. McCULLOH

Let J be a Dedekind ring, F its quotient field, F' a finite separable extension of F, and J' the integral closure of J in F'. It has been shown by Artin **(1)** that a necessary and sufficient condition that J' have an integral basis over J is that a certain ideal of F (namely, $\sqrt{(D/\Delta)}$, where D is the discriminant of the extension and Δ is the discriminant of an arbitrary basis of the extension) should be principal. More generally, he showed that if $\mathfrak{A}$ is an ideal of F', then a necessary and sufficient condition that $\mathfrak{A}$ have a module basis over J is that $N(\mathfrak{A})\sqrt{(D/\Delta)}$ should be principal.

Mann **(5)** has found a useful explicit form for the integral basis in the case that F' is a quadratic extension of F and an integral basis exists. In the same paper, he showed that a necessary and sufficient condition that F possess a quadratic extension without an integral basis is that F contain ideals which are not principal.

In this paper, results similar to those of Mann are proved. We consider Kummer extensions of prime degree l (i.e., extensions of the form $F' = F(\sqrt[l]{\mu})$, where it is assumed that F contains a primitive lth root of unity ζ). It is assumed throughout that F is locally perfect at the divisors of l (i.e., if a prime $\mathfrak{p}$ of F divides l, then the residue class field $F_{\mathfrak{p}}$ has no inseparable extensions). (This condition is easily seen to be satisfied if F is an algebraic number field, an algebraic function field, or any field of finite characteristic. Whether it is true of all Dedekind fields is not known to the author.)

First, an explicit construction is given for a module basis of an ideal $\mathfrak{A}$ of F' when such exists. This construction involves arbitrary choices only in the ground field F. In analogy with the second result of Mann, it is shown that if F is an algebraic number field, a necessary and sufficient condition for F to possess a Kummer extension of odd prime degree l without an integral basis is that F should possess an ideal $\mathfrak{a}$ such that $\mathfrak{a}^{\frac{1}{2}(l-1)}$ is not a principal ideal.

The construction of the module basis will be carried out in full for an odd prime l. The case $l = 2$ is similar and the necessary changes will be noted at the end. Let $\mathfrak{A}$ be an ideal of F' and suppose $N(\mathfrak{A})D^{\frac{1}{2}} = (\alpha)$, where $\alpha \in F$. (This is the form that Artin's condition takes for extensions of odd degree.) Now, $\alpha_i = \alpha(\sqrt[l]{\mu})^i$ $(i = 0, \ldots, l-1)$ are elements of $\mathfrak{A}$ having

$$(|\alpha_i^{(j)}|) = (\alpha)^l[(1-\zeta)^l(\mu)]^{\frac{1}{2}(l-1)}.$$

Received February 4, 1963. This paper includes parts of the author's Ph.D. thesis. The author wishes to thank Professor Mann for his encouragement and many suggestions.

https://doi.org/10.4153/CJM-1963-073-8 Published online by Cambridge University Press

(We may assume, of course, that μ is an integer.) Let

$$(\beta) = \frac{(|\alpha_i^{(j)}|)}{(\alpha)} = (\alpha)^{l-1}[(1-\zeta)^l(\mu)]^{\frac{1}{2}(l-1)},$$

where $\beta \in F$. By (**5**, Theorem 1, Corollary), we must find ω_i $(i = 0, \ldots, l-1)$ in $\mathfrak{A}$ so that

$$(|\omega_j^{(i)}|) = \frac{(|\alpha_j^{(i)}|)}{(\beta)} = (\alpha).$$

Lemma 1. *Suppose we have numbers* $\gamma_m \in \mathfrak{A}$ $(m = 0, \ldots, l-1)$ *where* $|\gamma_j^{(i)}| = |\alpha_j^{(i)}|$. *Suppose also that we have ideals* $\mathfrak{b}_m$ $(m = 0, \ldots, l-1)$ *in* F *such that*

$$\prod_{m=0}^{l-1} \mathfrak{b}_m = (\beta)$$

and that $\gamma_m \equiv 0$ $(\mathfrak{b}_m\mathfrak{A})$ $(m = 0, \ldots, l-1)$. *Then a module basis for* $\mathfrak{A}$ *over* F *exists.*

Proof. We construct a module basis $(\omega_0, \ldots, \omega_{l-1})$ given by

$$[\omega_0, \ldots, \omega_{l-1}] = [\gamma_0, \ldots, \gamma_{l-1}] \begin{bmatrix} a_0 & a_1 & \ldots & & a_{l-1} \\ c_1 & d_1 & & & \\ & c_2 & d_2 & & \\ & & \ddots & \ddots & \\ & & & c_{l-1} & d_{l-1} \end{bmatrix}$$

where the a's, c's, and d's are elements of F yet to be determined and the rest of the matrix is filled in with zeros. Let c_i, d_i $(i = 1, \ldots, l-1)$ be chosen so that $(c_i) = \mathfrak{c}_i/\mathfrak{b}_i$ and $(d_i) = \mathfrak{d}_i/\mathfrak{b}_i$ where $\mathfrak{c}_i$ $(i = 1, \ldots, l-1)$ and $\mathfrak{d}_i$ $(i = 1, \ldots, l-1)$ are relatively prime in pairs. Let $(a_i) = (a_i')\,\mathfrak{f}_i/\mathfrak{b}_0$ $(i = 0, \ldots, l-1)$ where the $\mathfrak{f}$'s are prime to each other and to all the $\mathfrak{c}$'s and $\mathfrak{d}$'s and where the a_i' are yet to be determined. Let A_i be the complementary minor of a_i. Then

$$a_iA_i = a_i\left(\prod_{j=1}^{i} c_j\right)\left(\prod_{j=i+1}^{l-1} d_j\right) = a_i'\beta_i/\beta$$

where

$$(\beta_i) = \mathfrak{f}_i\left(\prod_{j=1}^{i} \mathfrak{c}_j\right)\left(\prod_{j=i+1}^{l-1} \mathfrak{d}_j\right).$$

Also, $(\beta_0, \beta_1, \ldots, \beta_{l-1}) = (1)$, for indeed

$$(\beta_0, \beta_{l-1}) = \left(\mathfrak{f}_0\left(\prod_{j=1}^{l-1} \mathfrak{d}_j\right), \mathfrak{f}_{l-1}\left(\prod_{j=1}^{l-1} \mathfrak{c}_j\right)\right) = (1).$$

https://doi.org/10.4153/CJM-1963-073-8 Published online by Cambridge University Press

Hence, we may choose $a_0', \ldots, a_{l-1}'$ in J such that

$$\sum_{i=0}^{l-1} (-1)^i a_i' \beta_i = 1.$$

Then

$$\begin{vmatrix} a_0 & a_1 \ldots & & & a_{l-1} \\ c_1 & d_1 & & & \\ & c_2 & d_2 & & \\ & & \ddots & \ddots & \\ & & & c_{l-1} & d_{l-1} \end{vmatrix} = \sum_{i=0}^{l-1} (-1)^i a_i A_i = (1/\beta) \sum_{i=0}^{l-1} (-1)^i a_i' \beta_i = (1/\beta).$$

Hence $(|\omega_j^{(i)}|) = (1/\beta)(|\gamma_j^{(i)}|) = (\alpha) = N(\mathfrak{A})D^{\frac{1}{2}}$. Furthermore, $\omega_i \in \mathfrak{A}$, since

$$\begin{aligned} \omega_0 &= a_0\gamma_0 + c_1\gamma_1, \\ \omega_i &= a_i\gamma_0 + d_i\gamma_i + c_{i+1}\gamma_{i+1} \qquad (i = 1, \ldots, l-2), \\ \omega_{l-1} &= a_{l-1}\gamma_0 + d_{l-1}\gamma_{l-1}, \end{aligned}$$

and since $\gamma_i \equiv 0 \ (\mathfrak{A}\mathfrak{b}_i)$ for each i. Hence, the ω_i are a module basis for $\mathfrak{A}$ over F.

We shall proceed by constructing the γ's and the $\mathfrak{b}$'s. To do this, it will be necessary to study in detail the prime factorization of (β). This study will be facilitated by grouping similar primes. The following trivial lemma will provide the structure.

LEMMA 2. *Suppose* (β), $\mathfrak{A}$, *and the* γ_m *of Lemma* 1 *can each be broken up into four corresponding parts, viz.*

$$(\beta) = \prod_{i=1}^{4} \mathfrak{h}_i, \qquad \mathfrak{h}_i \textit{ an ideal of } F,$$

$$\mathfrak{A} = \prod_{i=1}^{4} \mathfrak{H}_i, \qquad \mathfrak{H}_i \textit{ an ideal of } F',$$

$$\gamma_m \equiv 0\left(\prod_{i=1}^{4} \mathfrak{G}_{im}\right), \qquad \mathfrak{G}_{im} \textit{ an ideal of } F'.$$

Further, suppose for each m $(m = 0, \ldots, l-1)$ *and each* i $(i = 1, \ldots, 4)$ *we can find* $\mathfrak{g}_{im}$, *an ideal of* F *such that* $\mathfrak{g}_{im}\mathfrak{H}_i$ *divides* $\mathfrak{G}_{im}$ *and*

$$\prod_{m=0}^{l-1} \mathfrak{g}_{im} = \mathfrak{h}_i.$$

Then choosing

$$\mathfrak{b}_m = \prod_{i=1}^{4} \mathfrak{g}_{im},$$

the conditions of Lemma 1 *will be satisfied.*

The plan will be to determine the $\mathfrak{h}_i$, $\mathfrak{H}_i$, $\mathfrak{G}_{im}$, $\mathfrak{g}_{im}$, and γ_m.

https://doi.org/10.4153/CJM-1963-073-8 Published online by Cambridge University Press

Under the conditions on F and F', the different $\mathfrak{D}$ of F' over F is the greatest common divisor of the differents of integers in F'. Also, if $\mathfrak{P}$ is a prime of F', $\mathfrak{P} \mid \mathfrak{D}$ if and only if the prime $\mathfrak{p}$ of F corresponding to $\mathfrak{P}$ is ramified in F'. Indeed, since l is prime, $\mathfrak{P}^{\nu(l-1)} \| \mathfrak{D}$ where ν is the order of ramification of $\mathfrak{P}$. ($\mid$ means "divides" and $\|$ means "divides exactly.")

Now the decomposition in F' of primes in F is studied in **(3)** and the order of ramification of ramified primes is found in **(2)**. The proofs are carried out for algebraic number fields, but can be carried over almost verbatim to the case studied here. Following is a summary of these results.

Summary. We may assume $(\mu) = \mathfrak{b}'\mathfrak{b}^l$, where $\mathfrak{b}'$ is divisible by the lth power of no ideal and $\mathfrak{b}$ is relatively prime to any given ideal.

If $\mathfrak{p}|\mathfrak{b}'$, then $\mathfrak{p}$ is ramified in F'. If $\mathfrak{p} \nmid \mu$ and $\mathfrak{p} \nmid l$, then $\mathfrak{p}$ splits or remains prime in F' according as $\mu \equiv \xi^l(\mathfrak{p})$ has a solution $\xi \in J$ or not. If $\mathfrak{p} \nmid \mu$ and $\mathfrak{p} \mid l$, suppose $\mathfrak{p}^a \| (1 - \zeta)$. (Note $(l) = (1 - \zeta)^{l-1}$.) Consider the congruence $\mu \equiv \xi^l$. If this is solvable mod $\mathfrak{p}^{al+1}$, then $\mathfrak{p}$ splits. If it is solvable mod $\mathfrak{p}^{al}$ but not mod $\mathfrak{p}^{al+1}$, then $\mathfrak{p}$ stays prime. If it is not solvable mod $\mathfrak{p}^{al}$, then $\mathfrak{p}$ is ramified. In the latter case, let k be the highest power of $\mathfrak{p}$ modulo which the congruence is solvable. Then $(k, l) = 1$ and $k < al$.

If $\mathfrak{p}$ is ramified, suppose $\mathfrak{p}^a \| (1 - \zeta)$. ($a$ may be zero.) If $\mathfrak{p}|\mathfrak{b}'$, the order of ramification is $al + 1$. If $\mathfrak{p} \nmid \mu$, the order of ramification is $al - k + 1$.

For the purposes of this proof, we shall assume $\mathfrak{b}$ relatively prime to $\mathfrak{b}'N(\mathfrak{A})(1 - \zeta)$. Also, let $\mathfrak{A} = \mathfrak{a}\mathfrak{A}'$, where $\mathfrak{a}$ is an ideal of F and $\mathfrak{A}'$ is an ideal of J' divisible by no ideal of J.

Let $\mathfrak{p}_i$ $(1 \leqslant i \leqslant n)$ be the distinct primes of F appearing as factors of $\mathfrak{b}'N(\mathfrak{A}')(1 - \zeta)$. We classify these primes according to the following table:

	$\mathfrak{p}_i \mid \mathfrak{b}'$	$\mathfrak{p}_i \mid (1 - \zeta)$	$\mathfrak{p}_i \mid N(\mathfrak{A}')$	Prime factors of $\mathfrak{p}_i$ in F'
$(1 \leqslant i \leqslant r)$	Yes	Perhaps	Perhaps	$(\mathfrak{P}_i{}^l)$
$(r < i \leqslant s)$	No	Yes	Perhaps	$\mathfrak{P}_i{}^l$
$(s < i \leqslant t)$	(No)	Yes	(No)	$\mathfrak{p}_i$
$(t < i \leqslant u)$	(No)	Yes	Perhaps	$\mathfrak{P}_i{}^{(1)} \ldots \mathfrak{P}_i{}^{(l)}$
$(u < i \leqslant n)$	No	No	(Yes)	$(\mathfrak{P}_i{}^{(1)} \ldots \mathfrak{P}_i{}^{(l)})$

Entries in parentheses follow from the other entries by the summary or by the fact that $N(\mathfrak{A}')$ can be divisible only by primes which split or are ramified in F'.

We now define integers a_i, k_i, b_i, and b_{ij}. Let

$$(1 - \zeta) = \prod_{i=1}^{n} \mathfrak{p}_i^{a_i}.$$

https://doi.org/10.4153/CJM-1963-073-8 Published online by Cambridge University Press

(Note: a_i may be zero for $1 \leqslant i \leqslant r$ and $a_i = 0$ for $u < i \leqslant n$.) Let

$$\mathfrak{b}' = \prod_{i=1}^{r} \mathfrak{p}_i^{k_i}.$$

For $r < i \leqslant s$, let k_i be as in the Summary. Let

$$N(\mathfrak{A}') = \left(\prod_{i=1}^{s} \mathfrak{p}_i^{b_i}\right)\left(\prod_{i=t+1}^{n} \mathfrak{p}_i^{b_i}\right), \qquad \mathfrak{A}' = \left(\prod_{i=1}^{s} \mathfrak{P}_i^{b_i}\right)\left(\prod_{i=t+1}^{n} \mathfrak{P}_i^{(1)b_{i1}} \cdots \mathfrak{P}_i^{(l)b_{il}}\right)$$

where for $1 \leqslant i \leqslant s, 0 \leqslant b_i < l$ and for $t < i \leqslant n$, the conjugates are arranged so that $b_{i1} \geqslant b_{i2} \geqslant \ldots \geqslant b_{il} = 0$. (Thus the automorphism ${}^l\sqrt{\mu} \rightarrow \zeta({}^l\sqrt{\mu})$ does not necessarily carry $\mathfrak{P}_i^{(1)}$ into $\mathfrak{P}_i^{(2)}$.) Note that $b_{i1} + \ldots + b_{il} = b_i$.

Then

$$\mathfrak{A} = \prod_{i=1}^{4} \mathfrak{H}_i$$

where

$$\mathfrak{H}_1 = \mathfrak{a},$$

$$\mathfrak{H}_2 = (1),$$

$$\mathfrak{H}_3 = \prod_{i=t+1}^{n} \mathfrak{P}_i^{(1)b_{i1}} \cdots \mathfrak{P}_i^{(l)b_{il}},$$

$$\mathfrak{H}_4 = \prod_{i=1}^{s} \mathfrak{P}_i^{b_i}.$$

Now, by the Summary,

$$\mathfrak{D} = \left[\left(\prod_{i=1}^{r} \mathfrak{P}_i^{a_i l+1}\right)\left(\prod_{i=r+1}^{s} \mathfrak{P}_i^{a_i l-k_i+1}\right)\right]^{l-1}.$$

Since $D = N(\mathfrak{D})$,

$$D^{\frac{1}{2}} = \left[\left(\prod_{i=1}^{r} \mathfrak{p}_i^{a_i l+1}\right)\left(\prod_{i=r+1}^{s} \mathfrak{p}_i^{a_i l-k_i+1}\right)\right]^{\frac{1}{2}(l-1)}.$$

Hence

$$(\beta) = (\alpha)^{l-1}[(1 - \zeta)^l(\mu)]^{\frac{1}{2}(l-1)} =$$

$$(\mathfrak{a}^l N(\mathfrak{A}')D^{\frac{1}{2}})^{l-1}\left[\left(\prod_{i=1}^{u} \mathfrak{p}_i^{a_i l}\right)\left(\prod_{i=1}^{r} \mathfrak{p}_i^{k_i}\right)(\mathfrak{b}^l)\right)\right]^{\frac{1}{2}(l-1)} = \prod_{i=1}^{4} \mathfrak{h}_i,$$

where

$$\mathfrak{h}_1 = (\mathfrak{a}^{l-1}D^{\frac{1}{2}})^l,$$

$$\mathfrak{h}_2 = \left[\left(\prod_{i=s+1}^{n} \mathfrak{p}_i^{a_i}\right)\mathfrak{b}\right]^{\frac{1}{2}l(l-1)},$$

$$\mathfrak{h}_3 = \prod_{i=t+1}^{n} \mathfrak{p}_i^{b_i(l-1)}$$

$$\mathfrak{h}_4 = \prod_{i=1}^{s} \mathfrak{p}_i^{\frac{1}{2}(k_i-1)(l-1)+b_i(l-1)}.$$

https://doi.org/10.4153/CJM-1963-073-8 Published online by Cambridge University Press

We next define the $\mathfrak{G}_{im}$. The reason for the definitions will become clear when the γ_m are defined. Let, for $m = 0, \ldots, l-1$,

$$\mathfrak{G}_{1m} = \mathfrak{a}^l D^{\frac{1}{2}},$$

$$\mathfrak{G}_{2m} = \left[\left(\prod_{i=s+1}^{n} \mathfrak{p}_i^{a_i}\right)\mathfrak{b}\right]^m,$$

$$\mathfrak{G}_{3m} = \prod_{i=t+1}^{n} \mathfrak{p}_i^{b_i}\mathfrak{P}_i^{(1)b_{i1}} \ldots \mathfrak{P}_i^{(m)b_{im}},$$

$$\mathfrak{G}_{4m} = \prod_{i=1}^{s} \mathfrak{p}_i^{b_i}\mathfrak{P}_i^{mk_i}.$$

Preparatory to defininining the $\mathfrak{g}_{im}$, we recall certain combinatorial facts by the following lemma.

Lemma 3. *Let $(k, l) = 1$. Then*

$$\sum_{m=0}^{l-1} [km/l] = (k-1)(l-1)/2,$$

where $[x]$ stands for the greatest integer $\leqslant x$. Let b be an integer satisfying $0 \leqslant b < l$. Let $\epsilon_m = 1$ or 0 according as $mk - [mk/l]l < b$ or $\geqslant b$. Then

$$\sum_{m=0}^{l-1} \epsilon_m = b.$$

Proof. The numbers $0, 1, 2, \ldots, l-1$ are a complete residue system mod l, and hence the numbers $0\cdot k, 1\cdot k, 2\cdot k, \ldots, (l-1)\cdot k$ are also. Thus, as m runs through $0, 1, \ldots, l-1$, so do the numbers $r_m = mk - [mk/l]l$. Since exactly b of these numbers are less than b, $\epsilon_m = 1$ for exactly b of the m's, which proves the second part of the lemma. Also

$$\sum_{m=0}^{l-1} [mk/l]l = \left(\sum_{m=0}^{l-1} mk\right) - \left(\sum_{m=0}^{l-1} r_m\right) = kl(l-1)/2 - l(l-1)/2,$$

whence the first part of the lemma follows.

We now define the $\mathfrak{g}_{im}$ and verify that they have the desired properties relative to the $\mathfrak{G}_{im}$, $\mathfrak{H}_i$, and $\mathfrak{h}_i$.

Let $\mathfrak{g}_{1m} = \mathfrak{a}^{l-1}D^{\frac{1}{2}}$. Then $\mathfrak{g}_{1m}\mathfrak{H}_1 = \mathfrak{a}^l D^{\frac{1}{2}} = \mathfrak{G}_{1m}$. Also

$$\prod_{m=0}^{l-1} \mathfrak{g}_{1m} = \mathfrak{a}^{l(l-1)}D^{\frac{1}{2}l} = \mathfrak{h}_1.$$

Let

$$\mathfrak{g}_{2m} = \left[\left(\prod_{i=s+1}^{n} \mathfrak{p}_i^{a_i}\right)\mathfrak{b}\right]^m.$$

Then $\mathfrak{g}_{2m}\mathfrak{H}_2 = \mathfrak{G}_{2m}$. Also

https://doi.org/10.4153/CJM-1963-073-8 Published online by Cambridge University Press

$$\prod_{m=0}^{l-1} \mathfrak{g}_{2m} = \left[\left(\prod_{i=s+1}^{n} \mathfrak{p}_i^{a_i}\right)\mathfrak{b}\right]^{\frac{1}{2}l(l-1)} = \mathfrak{h}_2$$

since

$$\sum_{m=0}^{l-1} m = l(l-1)/2.$$

Let

$$\mathfrak{g}_{3m} = \prod_{i=t+1}^{n} \mathfrak{p}_i^{b_i - b_{i,m+1}}.$$

Then

$$\mathfrak{G}_{3m}/\mathfrak{g}_{3m} = \prod_{i=t+1}^{n} \mathfrak{P}_i^{(1)b_{i1}}\mathfrak{P}_i^{(2)b_{i2}} \dots \mathfrak{P}_i^{(m)b_{im}}\mathfrak{p}_i^{b_{i,m+1}}$$

is divisible by

$$\prod_{i=t+1}^{n} \mathfrak{P}_i^{(1)b_{i1}} \dots \mathfrak{P}_i^{(l)b_{il}} = \mathfrak{H}_3$$

since $b_{i1} \geqslant b_{i2} \geqslant \dots \geqslant b_{il} = 0$. Also

$$\prod_{m=0}^{l-1} \mathfrak{g}_{3m} = \prod_{i=t+1}^{n} \mathfrak{p}_i^{b_i(l-1)} = \mathfrak{h}_3,$$

since

$$\sum_{m=0}^{l-1} (b_i - b_{i,m+1}) = lb_i - (b_{i1} + \dots + b_{il}) = lb_i - b_i = b_i(l-1).$$

Finally, let

$$\mathfrak{g}_{4m} = \prod_{i=1}^{s} \mathfrak{p}_i^{b_i - \epsilon_{im} + [mk_i/l]},$$

where $\epsilon_{im} = 1$ or 0 according as $mk_i - [mk_i/l]l < b_i$ or $\geqslant b_i$. Now

$$\mathfrak{G}_{4m} = \prod_{i=1}^{s} \mathfrak{p}_i^{b_i}\mathfrak{P}_i^{mk_i} = \prod_{i=1}^{s} \mathfrak{p}_i^{b_i + [mk_i/l]}\mathfrak{P}_i^{mk_i - [mk_i/l]\,l}.$$

Hence

$$\mathfrak{G}_{4m}/\mathfrak{g}_{4m} = \prod_{i=1}^{s} \mathfrak{P}_i^{mk_i - [mk_i/l]\,l}\mathfrak{p}_i^{\epsilon_{im}}$$

is divisible by

$$\mathfrak{H}_4 = \prod_{i=1}^{s} \mathfrak{P}_i^{b_i}.$$

For since $b_i < l$, $\mathfrak{P}_i^{b_i} | \mathfrak{p}_i^{\epsilon_{im}}$ unless $\epsilon_{im} = 0$. But then $\mathfrak{P}_i^{b_i} | \mathfrak{P}_i^{mk_i - [mk_i/l]\,l}$. Also

$$\prod_{m=0}^{l-1} \mathfrak{g}_{4m} = \prod_{i=1}^{s} \mathfrak{p}_i^{b_i(l-1) + \frac{1}{2}(k_i-1)(l-1)} = \mathfrak{h}_4,$$

since, by Lemma 3,

$$\sum_{m=0}^{l-1} (b_i - \epsilon_{im} + [mk_i/l]) = lb_i - b_i + ((k_i - 1)(l - 1)/2).$$

The final step is to define the γ_m and verify that $|\gamma_j^{(i)}| = |\alpha_j^{(i)}|$ and that

$$\gamma_m \equiv 0\left(\prod_{i=1}^{4} \mathfrak{G}_{im}\right).$$

LEMMA 4. *For every j $(1 \leqslant j \leqslant l - 1)$ we have an integer η_j in F such that $({}^{l}\sqrt{\mu} - \eta_j)$ is divisible by the ideal*

$$\left(({}^{l}\sqrt{\mu})\left(\prod_{i=r+1}^{s} \mathfrak{P}_i^{ki}\right)\left(\prod_{i=s+1}^{t} \mathfrak{p}_i^{ai}\right)\left(\prod_{i=t+1}^{n} \mathfrak{p}_i^{ai}\mathfrak{P}^{(j)bij}\right)\right).$$

Proof. First, we show the existence of ξ's (integers in F) such that

(A) $\quad {}^{l}\sqrt{\mu} \equiv \xi_i\ (\mathfrak{P}_i^{k_i}) \qquad (r < i \leqslant s),$

(B) $\quad {}^{l}\sqrt{\mu} \equiv \xi_i\ (\mathfrak{p}_i^{a_i}) \qquad (s < i \leqslant t),$

(C) $\quad {}^{l}\sqrt{\mu} \equiv \xi_{ij}\ (\mathfrak{p}_i^{a_i}\mathfrak{P}_i^{(j)b_{ij}}) \qquad (t < i \leqslant n)$ and $(1 \leqslant j \leqslant l - 1).$

To verify (A), let $\mathfrak{p}$ be any one of the $\mathfrak{p}_i$ $(r < i \leqslant s)$. By the Summary, we can find an integer $\xi \in F$ such that $\mathfrak{p}^k||(\mu - \xi^l)$. Suppose $\mathfrak{P}^{k'}||({}^{l}\sqrt{\mu} - \xi)$, Then the same is true for all the conjugates $\zeta^j({}^{l}\sqrt{\mu}) - \xi$, whence

$$\mathfrak{p}^{k'} = \mathfrak{P}^{k'l}||N({}^{l}\sqrt{\mu} - \xi) = (\mu - \xi^l).$$

Hence $k' = k$ and ${}^{l}\sqrt{\mu} \equiv \xi\ (\mathfrak{P}^k)$.

To verify (B), let $\mathfrak{p}$ be any one of the $\mathfrak{p}_i$ $(s < i \leqslant t)$. By the Summary, we can find an integer $\xi \in F$ such that $\mathfrak{p}^{al}||(\mu - \xi^l)$. If $\mathfrak{p}^{a'}||({}^{l}\sqrt{\mu} - \xi)$, the same is true for all the conjugates, and so $\mathfrak{p}^{a'l}||N({}^{l}\sqrt{\mu} - \xi) = (\mu - \xi^l)$. Hence $a' = a$ and ${}^{l}\sqrt{\mu} \equiv \xi\ (\mathfrak{p}^a)$.

To verify (C), let $\mathfrak{P}$ be any one of the $\mathfrak{P}_i^{(j)}$. Since $\mathfrak{P}$ is of degree one over F, J contains a complete system of residues mod $\mathfrak{P}$. Let $\pi \in J$, $\mathfrak{p}||\pi$. Then $\mathfrak{P}||\pi$. Hence, we have for any $b \geqslant 0$,

$${}^{l}\sqrt{\mu} \equiv a_0 + a_1\pi + \ldots + a_{a+b-1}\pi^{a+b-1}(\mathfrak{P}^{a+b}),$$

where the a's, and hence the entire right side, belong to J. Hence ${}^{l}\sqrt{\mu}-\xi\equiv 0$ $(\mathfrak{P}^{a+b})$. We must now show ${}^{l}\sqrt{\mu} - \xi \equiv 0\ (\mathfrak{P}^{(j)a})$ where $\mathfrak{P}^{(j)}$ is any conjugate of $\mathfrak{P}$. For some r, we have $\zeta^r({}^{l}\sqrt{\mu}) - \xi \equiv 0\ (\mathfrak{P}^{(j)a+b})$. But

$$({}^{l}\sqrt{\mu} - \xi) - (\zeta^r({}^{l}\sqrt{\mu}) - \xi) = (1 - \zeta^r)\ {}^{l}\sqrt{\mu} \equiv 0\ (1 - \zeta).$$

Hence ${}^{l}\sqrt{\mu} - \xi \equiv \zeta^r({}^{l}\sqrt{\mu}) - \xi\ (\mathfrak{p}^a)$ and so ${}^{l}\sqrt{\mu} - \xi \equiv 0\ (\mathfrak{P}^{(j)a})$. Hence ${}^{l}\sqrt{\mu} - \xi \equiv 0\ (\mathfrak{p}^a\mathfrak{P}^b)$.

Now, for each $1 \leqslant j \leqslant l - 1$, we may find, by the Chinese remainder theorem, an integer $\eta_j \in F$ such that

$$\eta_j \equiv \xi_i(\mathfrak{P}_i^{k_i}) \qquad (r < i \leqslant s),$$
$$\eta_j \equiv \xi_i(\mathfrak{p}_i^{a_i}) \qquad (s < i \leqslant t),$$

$$\eta_j \equiv \xi_{ij}\ (\mathfrak{p}_i^{a_i}\mathfrak{P}^{(j)b_{ij}}) \qquad (t < i \leqslant n),$$
$$\eta_j \equiv 0\ ({}^l\sqrt{\mu}).$$

Hence, ${}^l\sqrt{\mu} - \eta_j$ satisfies the required condition.

We define the γ's of Lemma 1 to be $\gamma_0 = \alpha$ and for $1 \leqslant m \leqslant l - 1$, $\gamma_m = \alpha({}^l\sqrt{\mu} - \eta_1)({}^l\sqrt{\mu} - \eta_2) \ldots ({}^l\sqrt{\mu} - \eta_m)$. Then, since

$$({}^l\sqrt{\mu}) = \mathfrak{b} \prod_{i=1}^{r} \mathfrak{P}_i^{k_i},$$

γ_m is divisible by

$$\alpha\mathfrak{b}^m\left(\prod_{i=1}^{s} \mathfrak{P}_i^{k_i m}\right)\left(\prod_{i=s+1}^{n} \mathfrak{p}_i^{a_i m}\right)\left(\prod_{i=t+1}^{n} \mathfrak{P}_i^{(1)b_{1i}} \ldots \mathfrak{P}_i^{(m)b_{im}}\right),$$

which is equal to

$$\prod_{i=1}^{4} \mathfrak{G}_{im}.$$

Now $|\alpha_j^{(i)}| = |\gamma_j^{(i)}|$ since the matrix $[\alpha_j^{(i)}]$ can be transformed into the matrix $[\gamma_j^{(i)}]$ by the following procedure. The columns are numbered $0, 1, \ldots, l - 1$. From each of the columns $1, \ldots, l - 1$, subtract η_1 times the preceding column starting with the last column and progressing to the first. Then from each of the columns $2, \ldots, l - 1$ subtract η_2 times the preceding column starting with the last column. Then from each of the columns $3, \ldots, l - 1$ subtract η_3 times the preceding column. Continue this process until the final step, which is to subtract η_{l-1} times the preceding column from column $l - 1$.

This completes the construction.

We conclude with the following theorem.

THEOREM. *Let F be an algebraic number field containing ζ, a primitive lth root of unity where l is an odd prime. A necessary and sufficient condition for F to possess an extension of type $F' = F({}^l\sqrt{\mu})$ without an integral basis is that F contain an ideal whose $(l - 1)/2$th power is not a principal ideal.*

Proof. The condition is clearly necessary since $D^{\frac{1}{2}}$ is the $(l - 1)/2$th power of an ideal.

Since F is an algebraic number field, every ideal class (absolute or mod $\mathfrak{m}$, where $\mathfrak{m}$ is any ideal in J) contains an infinite number of prime ideals. We may assume, thus, that there is a prime ideal $\mathfrak{p}$ not dividing $1 - \zeta$ whose $(l - 1)/2$th power is not principal. We consider two cases, first that there is an ideal whose $l(l - 1)/2$th power is not principal and second that the $l(l - 1)/2$th power of every ideal is principal.

Case 1. *Let* $\mathfrak{p}^{\frac{1}{2}l(l-1)}$ be non-principal, where $\mathfrak{p} \nmid (1 - \zeta)$. Let $\bar{\mathfrak{p}}$ be in the inverse class (mod $(1 - \zeta)^l$) of $\mathfrak{p}^l$. Then $\bar{\mathfrak{p}}\mathfrak{p}^l = (\mu)$, where $\mu \equiv 1\ ((1 - \zeta)^l)$. Let $F' = F({}^l\sqrt{\mu})$. Then no primes dividing $(1 - \zeta)$ are ramified since for any such prime $\mathfrak{p}_1$, $\mu \equiv 1^l\,(\mathfrak{p}_1{}^{a_1 l})$. Hence, $D^{\frac{1}{2}} = (\bar{\mathfrak{p}})^{\frac{1}{2}(l-1)}$. But $D^{\frac{1}{2}}$ is not principal. For otherwise $(\mu)^{\frac{1}{2}(l-1)} = \bar{\mathfrak{p}}^{\frac{1}{2}(l-1)}\mathfrak{p}^{\frac{1}{2}l(l-1)}$ would not be principal, by the assumption on $\mathfrak{p}$, and this is clearly a contradiction. Hence F' has no integral basis over F.

Case 2. Let $\mathfrak{p}^{\frac{1}{2}(l-1)}$ be non-principal with $\mathfrak{p} \nmid (1-\zeta)$. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_{l-1}$ be distinct primes in the same class mod $(1-\zeta)^l$ as $\mathfrak{p}$. Let $\bar{\mathfrak{p}}$ be in the inverse class mod $(1-\zeta)^l$ of $\mathfrak{p}$. Then $\mathfrak{p}_1\mathfrak{p}_2{}^2 \ldots \mathfrak{p}_{l-1}{}^{l-1}\bar{\mathfrak{p}}^{\frac{1}{2}l(l-1)} = (\mu)$, where $\mu \equiv 1$ $((1-\zeta)^l)$. Hence, as before, if $F' = F(\sqrt[l]{\mu})$, $D^{\frac{1}{2}} = (\mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_{l-1})^{\frac{1}{2}(l-1)}$. But $D^{\frac{1}{2}}$ is not principal. For $D^{\frac{1}{2}}$ is in the same class as $\mathfrak{p}^{\frac{1}{2}(l-1)(l-1)}$. And $\mathfrak{p}^{\frac{1}{2}(l-1)(l-1)}$ is not principal since $\mathfrak{p}^{\frac{1}{2}(l-1)(l-1)}\mathfrak{p}^{\frac{1}{2}(l-1)} = \mathfrak{p}^{\frac{1}{2}l(l-1)}$ is principal but $\mathfrak{p}^{\frac{1}{2}(l-1)}$ is not. Hence F' has no integral basis over F.

This completes the proof.

The construction of a module basis for an ideal can also be carried out for the case $l = 2$. In this case, the necessary and sufficient condition for the existence of a module basis is that $N(\mathfrak{A})D^{\frac{1}{2}} = (\alpha)$, where $\alpha \notin F$, but $\alpha^2 \in F$. The construction is similar to the case $l \neq 2$ but starts by letting $\alpha_0 = \alpha^2$ and $\alpha_1 = \alpha^2\sqrt{\mu}$.

Then $(|\alpha_j{}^{(i)}|) = (\alpha)^4(\sqrt{\mu})\ (2)$ and

$$(\beta) = \frac{(|\alpha_j{}^{(i)}|)}{(\alpha)} = (\alpha)^3(\sqrt{\mu})(2) \in F$$

since $\alpha = a\sqrt{\mu}$, where $a \in F$. Lemmas 1 and 2 remain unchanged as do the Summary, the classification of primes $\mathfrak{p}_i$ $(1 \leqslant i \leqslant n)$, and the definitions of a_i, k_i, b_i, and b_{ij}. Note that $k_i = 1$ for $1 \leqslant i \leqslant r$ and that k_i is odd for $1 \leqslant i \leqslant s$. Also, for $1 \leqslant i \leqslant s$, $b_i = 0$ or 1. And, for $t < i \leqslant n$, $b_{i1} = b_i$ and $b_{i2} = 0$.

The $\mathfrak{H}_i$ remain the same. The different can be written:

$$\mathfrak{D} = D^{\frac{1}{2}} = \left(\prod_{i=1}^{r} \mathfrak{p}_i{}^{a_i}\mathfrak{P}_i\right)\left(\prod_{i=r+1}^{s} \mathfrak{p}_i{}^{a_i-[k_i/2]}\right).$$

We redefine

$$\mathfrak{h}_1 = \mathfrak{a}^6 D^2,$$

$$\mathfrak{h}_2 = \left(\prod_{i=s+1}^{n} \mathfrak{p}_i{}^{a_i}\right)\mathfrak{b},$$

$$\mathfrak{h}_3 = \prod_{i=t+1}^{n} \mathfrak{p}_i{}^{3b_i},$$

$$\mathfrak{h}_4 = \prod_{i=1}^{s} \mathfrak{p}_i{}^{3b_i+[k_i/2]}.$$

So

$$(\beta) = \prod_{i=1}^{4} \mathfrak{h}_i.$$

The $\mathfrak{G}_{im}$ are redefined:

$$\begin{aligned} \mathfrak{G}_{10} &= \mathfrak{a}^4 D, & \mathfrak{G}_{11} &= \mathfrak{a}^4 D, \\ \mathfrak{G}_{20} &= (1), & \mathfrak{G}_{21} &= \Big(\prod_{i=s+1}^{n} \mathfrak{p}_i^{ai}\Big)\mathfrak{b}, \\ \mathfrak{G}_{30} &= \prod_{i=t+1}^{n} \mathfrak{p}_i^{2bi}, & \mathfrak{G}_{31} &= \prod_{i=t+1}^{n} \mathfrak{p}_i^{2bi}\mathfrak{P}_i^{(1)bi1} \\ \mathfrak{G}_{40} &= \prod_{i=1}^{s} \mathfrak{p}_i^{2bi}, & \mathfrak{G}_{41} &= \prod_{i=1}^{s} \mathfrak{p}_i^{2bi}\mathfrak{P}_i^{ki}. \end{aligned}$$

The $\mathfrak{g}_{im}$ are redefined:

$$\begin{aligned} \mathfrak{g}_{10} &= \mathfrak{a}^3 D, & \mathfrak{g}_{11} &= \mathfrak{a}^3 D, \\ \mathfrak{g}_{20} &= (1), & \mathfrak{g}_{21} &= \Big(\prod_{i=s+1}^{n} \mathfrak{p}_i^{ai}\Big)\mathfrak{b}, \\ \mathfrak{g}_{30} &= \prod_{i=t+1}^{n} \mathfrak{p}_i^{bi}, & \mathfrak{g}_{31} &= \prod_{i=t+1}^{n} \mathfrak{p}_i^{2bi}, \\ \mathfrak{g}_{40} &= \prod_{i=1}^{s} \mathfrak{p}_i^{bi}, & \mathfrak{g}_{41} &= \prod_{i=1}^{s} \mathfrak{p}_i^{2bi+[ki/2]}, \end{aligned}$$

and have the desired properties relative to the $\mathfrak{G}_{im}$, $\mathfrak{h}_i$, and $\mathfrak{H}_i$. Lemma 4 also carries over and we let $\gamma_0 = \alpha^2$, and $\gamma_1 = \alpha^2(\sqrt{\mu} - \eta_1)$, and we can easily verify that

$$\gamma_m \equiv 0\Big(\prod_{i=1}^{4} \mathfrak{G}_{im}\Big)$$

and $(|\alpha_j^{(i)}|) = (|\gamma_j^{(i)}|)$.

References

1. E. Artin, *Questions de base minimale dans la théorie des nombres algébriques*, Algèbre et Théorie des Nombres, Colloques Internationaux du Centre National de la Recherche Scientifique, No. 24, pp. 19–20 (Paris, 1950).
2. H. S. Butts and H. B. Mann, *Corresponding residue systems in algebraic number fields*, Pacific J. Math., *6* (1956), 211–224.
3. E. Hecke, *Vorlesungen ueber die Theorie der algebraischen Zahlen* (New York, 1948).
4. H. B. Mann, *Introduction to algebraic number theory* (Columbus, 1955).
5. ——— *On integral bases*, Proc. Amer. Math. Soc., *9* (1958), 167–172.

The University of Illinois,
Urbana, Illinois

https://doi.org/10.4153/CJM-1963-073-8 Published online by Cambridge University Press